Colleagues,

I have some exciting news! Ms. Kim Zetter, author of the book: *Countdown to Zero Day, Stuxnet and the Launch of the World’s First Digital Weapon*, is our guest speaker for the 18 July lunch meeting. She’s an award-winning investigative journalist who specializes in cybersecurity and national security, as well as privacy and civil liberties issues. I read her book some time ago, it’s excellent! I highly encourage everyone to read it. Top cybersecurity journalist Kim Zetter was among the first journalists to cover Stuxnet after its discovery and has also broken numerous stories over the years about WikiLeaks, NSA surveillance, and the hacker underground.

Please register ASAP (via our website) to meet and hear from this excellent guest speaker!

Please note that our lunch meeting (this month see Page 9) will once again be held at the Hewlett-Packard Enterprise (HPE) facility located at 305 South Rockrimmon Blvd. To ensure maximum attendance, we’re holding a lunch meeting in July. The dinner meeting is cancelled. Additional information will be on our website and in emails soon. Please note that the HP facility sits ~600 feet west off Rockrimmon.

As usual, lunch is free for members. Non-members may join us for this meeting by registering and paying $12 to help offset the cost for the lunch meal. Feel free to invite colleagues to join us, but please have them register and pay to attend.

Also, please note that registrations for this event will close two days prior to the event so we’ll have a good head count for our caterer.

**Peak Cyber is coming soon!**

Our Peak Cyber conference will be here soon – on 22-23 August. We have some excellent keynote speakers already confirmed:

- COL Robert McVay, Deputy CIO, MDA
- Dr. Meyerrose, The MeyerRose Group
- Dr. Joseph Mitola III, Chief Technologist, ENSCO Aerospace Sciences and Engineering Division, Fellow of the IEEE
- Ron Ross, Fellow, Computer Security Division, NIST
- Jeff Snyder, Jeff Snyder Cyber Recruiting & Coaching

(Continued on page 4)
The Wiretap Rooms

By Ryan Gallagher and Henrik Moltke, The Intercept, June 25, 2018

Federal agencies are so far unable to comply with a law banning Kaspersky Lab software from U.S. government networks by October, The Daily Beast has learned. Multiple divisions of the U.S. government are confronting the reality that code written by the Moscow-based security company is embedded deep within American infrastructure, in routers, firewalls, and other hardware—and nobody is certain how to get rid of it.

The secrets are hidden behind fortified walls in cities across the United States, inside towering, windowless skyscrapers and fortress-like concrete structures that were built to withstand earthquakes and even nuclear attack. Thousands of people pass by the buildings each day and rarely give them a second glance, because their function is not publicly known. They are an integral part of one of the world’s largest telecommunications networks – and they are also linked to a controversial National Security Agency surveillance program.

Atlanta, Chicago, Dallas, Los Angeles, New York City, San Francisco, Seattle, and Washington, D.C. In each of these cities, The Intercept has identified an AT&T facility containing networking equipment that transports large quantities of internet traffic across the United States and the world. A body of evidence – including classified NSA documents, public records, and interviews with several former AT&T employees – indicates that the buildings are central to an NSA spying initiative that has for years monitored billions of emails, phone calls, and online chats passing across U.S. territory.

The NSA considers AT&T to be one of its most trusted partners and has lauded the company’s “extreme willingness to help.” It is a collaboration that dates back decades. Little known, however, is that its scope is not restricted to AT&T’s customers. According to the NSA’s documents, it values AT&T not only because it “has access to information that transits the nation,” but also because it maintains unique relationships with other phone and internet providers. The NSA exploits these relationships for surveillance purposes, commandeering AT&T’s massive infrastructure and using it as a platform to covertly tap into communications processed by other companies.

Much has previously been reported about the NSA’s surveillance programs. But few details have been disclosed about the physical infrastructure that enables the spying. Last year, The Intercept highlighted a likely NSA facility in New York City’s Lower Manhattan. Now, we are revealing for the first time a series of other buildings across the U.S. that appear to serve a similar function, as critical parts of one of the world’s most powerful electronic eavesdropping systems, hidden in plain sight.

“It’s eye-opening and ominous the extent to which this is happening right here on American soil,” said Elizabeth Goitein, co-director of the Liberty and National Security Program at the Brennan Center for Justice. “It puts a face on surveillance that we could never think of before in terms of actual buildings and actual facilities in our own cities, in our own backyards.”

There are hundreds of AT&T-owned properties scattered across the U.S. The eight identified by The Intercept serve a specific function, processing AT&T customers’ data and also carrying large quantities of data from other internet providers. They are known as “backbone” and “peering” facilities.

While network operators would usually prefer to send data through their own networks, often a more direct and cost-efficient path is provided by other providers’ infrastructure. If one network in a specific area of the country is overloaded with data traffic, another operator with capacity to spare can sell or exchange bandwidth, reducing the strain on the congested region. This exchange of traffic is called “peering” and is an essential feature of the internet.

While network operators would usually prefer to send data through their own networks, often a more direct and cost-efficient path is provided by other providers’ infrastructure. If one network in a specific area of the country is overloaded with data traffic, another operator with capacity to spare can sell or exchange bandwidth, reducing the strain on the congested region. This exchange of traffic is called “peering” and is an essential feature of the internet.

Read the rest here:
It's been a dead month on the membership front. Our membership has dropped a little over the last several months to around the 475 mark as of the end of June. For the first time in the four plus years I’ve been involved with membership for the chapter, we enrolled no new members. As you’re going about your daily activities, please take the time to engage your colleagues, ask if they’re ISSA members, and if not take a couple of minutes to convince them of the value of becoming a member of our chapter. Word of mouth is our primary method of advertising. If you don’t take the time to tell people of our organization, folks won’t know all the advantages we bring to their professional life.

Renewals are also critical to maintaining our membership. If you are considering not renewing, please talk to me or one of the other board members to help us understand what we can do better to support our membership and retain you as active chapter members.

We have lots of upcoming activities scheduled between meetings, training and mini-seminars. Please watch the Newsletter, communications and eVites to ensure you stay aware of what’s going on in the chapter. Please continue to refer new members to the chapter. Referrals are a critical part of developing new members for ISSA. As always, if you have any membership questions don’t hesitate to contact me.

Thanks,

David Reed
Membership Committee Chairman
dreed54321@comcast.net

Update Your Profile!
Don’t forget to periodically logon to www.issa.org and update your personal information.
Many more speakers – and several cybersecurity training offerings – are also confirmed. Check out this site for more info and to register: https://www.fbcinc.com/e/csttf/. Please register now to guarantee your seat at the Peak Cyber – Cyber Security Training and Technology Forum (CSTTF)!!!

Colleen

Mentorship Committee Update

Next Mentorship Group Meeting will be in July. Thanks to all who attended last month's meeting. For more information about the program, please email Melissa Absher at mentorship@issa-cos.org.

Mission Statement

Mission Statement. Provide interested mentees at any stage of their information security career lifecycle with access to mentors who share their knowledge and experience in ensuring the confidentiality, integrity, and availability of information resources throughout a variety of industries.

Overview

The ISSA-COS Mentorship Program is designed to be mentee driven. Mentees determine the number of mentors they meet with depending on their questions, needs, and availability. The goal is to provide mentees with quality mentoring opportunities in a professional and problem solving environment. There will be group meetings quarterly for all mentors and mentees to meet, greet, and discuss information security. Individual meetings between mentees and mentors will be scheduled throughout the year determined by the mentee and mentor. Mentees and mentors are expected to prepare for individual meetings by writing down questions and discussion topics prior to the meeting. e-Mentoring is also an option for those who need remote options. Small group meetings to discuss specific topics and field trips to companies and organizations will be scheduled ad hoc.

https://issa-cos.org/mentorship-program/
The Information Systems Security Association (ISSA) - Colorado Springs Chapter will once again host the 8th Annual Peak Cyber - Cybersecurity Training & Technology Forum (CSTTF). Peak Cyber - CSTTF is set to convene from Wednesday August 22nd to Thursday, August 23rd, 2018 at the DoubleTree by Hilton, Colorado Springs, Colorado.

**Attendee Registration is now open:** There is no fee to attend Peak Cyber for all ISSA members, military, government, and contractor personnel with a .mil or .gov e-mail address. To pre-register visit www.fbcinc.com/csttf

**Exhibit and Sponsor opportunities are also still available.** Visit www.fbcinc.com/csttf for more information.

**Want to Speak at Peak Cyber?** We have a limited number of open sessions for available. Contact Dennis O’Neill at dennis@fbcdb.com about remaining speaking opportunities, or for general symposium questions.

---

**Keynote Speakers**

**Dr. Ron Ross,** Computer Scientist, NIST Fellow https://www.nist.gov/people/ronald-s-ross has confirmed that he will give the opening Keynote at the 8th Annual Peak Cyber – CSTTF Symposium www.fbcinc.com/csttf Colorado Springs, CO on August 22nd, 2018.

He will join **Dr. Dale W. Meyerrose,** Major General USAF Retired, President, MeyerRose Group, Stephen Coury, CISO, The City and County of Denver, Rich Schliep, CISO, Network Manager, Colorado Department of State, Tim McCain, CISO, City of Aurora, CO and many other thought leaders from Colorado and around the nation to address some of today’s most pressing cybersecurity threats and remediation strategies.
ISSA Nametags

Do you want an ISSA nametag for your very own to wear to meetings, conferences, and events? You can now order/pick up yours directly from:

Blue Ribbon Trophies & Awards

245 E Taylor St  (behind Johnny’s Navajo Hogan on North Nevada)

Colorado Springs

(719) 260-9911

Although their hours are officially Monday through Friday until 5:30 pm, they are occasionally in the shop on Saturdays. This is a small business so cash/check would be appreciated. Email wbusovsky@aol.com to order.

ISSA-COS NEWS
Who Should Attend?
IT Admins who are interested in cybersecurity, Ethical Hackers, Pen Testers. Attendees receive 8 CEU’s.

What is the Mobile Security Tool Kit?
EC-Council’s Mobile Security Toolkit (Better known as the STORM!) is a fully-loaded pen-test platform which comes equipped with a customized distro of Kali loaded onto a portable Raspberry Pi-based touchscreen device.

EC-Council rolled out the STORM as a mobile tool to enhance our certification course offerings by giving online asynchronous students a mobile training option. In this option, the video lectures are loaded directly onto the STORM.

What is the Mobile Security Tool Kit Workshop?
The course content was derived by pulling carefully selected modules from EC-Council’s Certified Network Defender (CND) and Certified Ethical Hacker (CEH) certification courses.

Course includes:
e-Book • Certificate of Attendance (.pdf) • STORM device keyboard • carry case • STORM T-shirt • STORM Sticker

Check out the videos:
Storm Device  Storm Workshop

TRAINING DATES
08/23/2018

PRICING
Retail Price: $999
15% discount for ISSA, AFCEA, and Government Ask your sales representative.

LOCATION
Doubletree Hotel
1775 E Cheyenne Mountain Blvd
Colorado Springs, CO

CONTACT
Michael Shivers
michael.shivers@eccouncil.org
(520) 526-9932

ABOUT EC-COUNCIL
EC-Council has been the world’s leading information security certification body since the launch of their flagship program, Certified Ethical Hacker (CEH), which created the ethical hacking industry in 2002. Since the launch of CEH, EC-Council has added industry-leading programs to their portfolio to cover all aspects of information security including EC-Council Certified Security Analyst (ECSA), Computer Hacking Forensics Investigator (CHFI), Certified Chief Information Security Officer (CISO), among others.
SANS IS COMING TO THE SPRINGS!

SEC560: Network Penetration Testing and Ethical Hacking

As a cybersecurity professional, you have a unique responsibility to find and understand your organization's vulnerabilities and to work diligently to mitigate them before the bad guys pounce. Are you ready? SEC560, the flagship SANS course for penetration testing, fully arms you to address this duty head-on.

THE MUST-HAVE COURSE FOR EVERY WELL-ROUNDED SECURITY PROFESSIONAL

With comprehensive coverage of tools, techniques, and methodologies for network penetration testing, SEC560 truly prepares you to conduct high-value penetration testing projects step-by-step and end-to-end. Every organization needs skilled information security personnel who can find vulnerabilities and mitigate their effects, and this entire course is specially designed to get you ready for that role. The course starts with proper planning, scoping and recon, then dives deep into scanning, target exploitation, password attacks, and web app manipulation, with over 30 detailed hands-on labs throughout. The course is chock full of practical, real-world tips from some of the world's best penetration testers to help you do your job safely, efficiently...and masterfully.

LEARN THE BEST WAYS TO TEST YOUR OWN SYSTEMS BEFORE THE BAD GUYS ATTACK

SEC560 is designed to get you ready to conduct a full-scale, high-value penetration test - and on the last day of the course you'll do just that. After building your skills in comprehensive and challenging labs over five days, the course culminates with a final full-day, real-world penetration test scenario. You'll conduct an end-to-end pen test, applying knowledge, tools, and principles from throughout the course as you discover and exploit vulnerabilities in a realistic sample target organization, demonstrating the knowledge you've mastered in this course.

EQUIPPING SECURITY ORGANIZATIONS WITH COMPREHENSIVE PENETRATION TESTING AND ETHICAL HACKING KNOW-HOW

You will learn how to perform detailed reconnaissance, studying a target's infrastructure by mining blogs, search engines, social networking sites, and other Internet and intranet infrastructures. Our hands-on labs will equip you to scan target networks using best-of-breed tools. We won’t just cover run-of-the-mill options and configurations, we’ll also go over the lesser known but super-useful capabilities of the best pen test toolsets available today. After scanning, you'll learn dozens of methods for exploiting target systems to gain access and measure real business risk. You'll dive deep into post-exploitation, password attacks, and web apps, pivoting through the target environment to model the attacks of real-world bad guys to emphasize the importance of defense in depth.

Go here for more information: https://www.sans.org/community/event/sec560-colorado-springs-54890
ISSA-COS July Monthly Meeting - Lunch Only


Don’t miss out on earning 2 free continuing education credits!

Don’t miss out on the opportunity to network with your cybersecurity peers!

Don’t miss out on the free food!

Hello Colleagues,

Please join us for our monthly meeting for Lunch at HP Enterprise (HPE) off S. Rockrimmon.

Lunch – July 18th (Wednesday 11:00-1:00)

The meeting presentation is:


An award-winning investigative journalist who specializes in cybersecurity and national security, as well as privacy and civil liberties issues.

Members are free and Guests are $12.00.

Reservations close Monday, July 16th, 1100am.

Friendly Reminder: No August Member Monthly Meeting due to our Annual CSTTF.
CRACKING THE CRYPTO WAR

By Steven Levy, Wired, April 25, 2018

On December 2, 2015, a man named Syed Rizwan Farook and his wife, Tashfeen Malik, opened fire on employees of the Department of Public Health in San Bernardino, California, killing 14 people and injuring 22 during what was supposed to be a staff meeting and holiday celebration. The shooters were tracked down and killed later in the day, and FBI agents wasted no time trying to understand the motivations of Farook and to get the fullest possible sense of his contacts and his network. But there was a problem: Farook’s iPhone 5c was protected by Apple’s default encryption system. Even when served with a warrant, Apple did not have the ability to extract the information from its own product.

The government filed a court order, demanding, essentially, that Apple create a new version of the operating system that would enable it to unlock that single iPhone. Apple defended itself, with CEO Tim Cook framing the request as a threat to individual liberty.

“We have a responsibility to help you protect your data and protect your privacy,” he said in a press conference. Then-FBI chief James Comey reportedly warned that Cook’s attitude could cost lives. “I just don’t want to get to a day where people look at us with tears in their eyes and say, ‘My daughter is missing and you have her cell phone—what do you mean you can’t tell me who she was - texting before she disappeared?’ ” The controversy over Farook’s iPhone reignited a debate that was known in the 1990s as the Crypto Wars, when the government feared the world was “going dark” and tried—and ultimately failed—to impede the adoption of technologies that could encode people’s information. Only this time, with super-computers in everybody’s pockets and the endless war on terror, the stakes were higher than ever.

A few months after the San Bernardino shooting, President Obama sat for an interview at the South by Southwest conference and argued that government officials must be given some kind of shortcut—or what’s known as exceptional access—to encrypted content during criminal and antiterrorism investigations. “My conclusion so far is that you cannot take an absolutist view on this,” he said. “If the tech community says, ‘Either we have strong, perfect encryption or else it’s Big Brother and an Orwellian world’—what you’ll find is that after something really bad happens, the politics of this will swing and it will become sloppy and rushed, and it will go through Congress in ways that have not been thought through. And then you really will have dangers to our civil liberties.”

In typical Obama fashion, the president was leaning toward a compromise, a grand bargain between those who insist that the NSA and FBI need all the information they can get to monitor potential terrorists or zero in on child abusers and those who believe building any sort of exceptional access into our phones would be a fast track to a totalitarian surveillance state. And like so many of Obama’s proposed compromises, this one went nowhere. To many cryptographers, there was simply no way that companies like Apple and Google could provide the government with legal access to customer data without compromising personal privacy and even national security. Exceptional access was a form of technology, after all, and any of its inevitable glitches, flaws, or bugs could be exploited to catastrophic ends. To suggest otherwise, they argued, was flat wrong. Flat-Earth wrong. Which was, as any good engineer or designer knows, an open invitation for someone to prove them wrong.

This past January Ray Ozzie took a train from his home in Massachusetts to New York City for a meeting in a conference room of the Data Science Institute at Columbia University. The 14th-floor aerie was ringed by wide windows and looked out on a clear but chilly day. About 15 people sat around the conference table, most of them middle-aged academics—people from the law school, scholars in government policy, and computer scientists, including cryptographers and security specialists—nibbling on a light lunch while waiting for Ozzie’s presentation to begin.

Jeannette Wing—the host of the meeting and a former corporate VP of Microsoft Research who now heads the Data Science Institute—introduced Ozzie to the group. In the invitation to this “private, informal session,” she’d referenced his background, albeit briefly. Ozzie was once chief technical officer at Microsoft as well as its chief software architect; posts he had assumed after leaving IBM, where he’d gone to work after the company had purchased a product he created, Lotus Notes. Packed in that sentence was the stuff of legend: Notes was a groundbreaking product that rocketed businesses into internet-style communications when the internet was barely a thing. The only other person who ever held the chief software architect post at Microsoft was Bill Gates, and Ozzie had also helped create the company’s cloud business.

Read the rest here:
https://www.wired.com/story/crypto-war-clear-encryption/
Cybercriminals looking to maximize their investments are using evermore sophisticated software techniques and increasingly aggressive steps against their fellow malware authors. Those are among the conclusions by researchers at Deep Instinct about a new strain of malware found within the last two months.

The new malware, dubbed Mylobot, pulls together a variety of techniques to gain a foothold and remain undiscovered. Among the strategies employed are:

- Anti-VM techniques
- Anti-sandbox techniques
- Anti-debugging techniques
- Wrapping internal parts with an encrypted resource file
- Code injection
- Process hollowing (a technique where an attacker creates a new process in a suspended state and replaces its image with the one that is to be hidden)
- Reflective EXE (executing EXE files directly from memory, without having them on disk)
- A 14-day delay before accessing its C&C servers.

"On a daily basis we come across dozens of highly sophisticated samples, but this one is a unique collection of highly advanced techniques," says Arik Solomon, vice president of R&D at Deep Instinct. "Each of the techniques is known and used by a few malicious samples, but the combination is unique."

Solomon noted that Mylobot — named for a researcher's dog — is a downloader: It can be purposed to download and install any type of payload, from spambot or DDoS engine to keylogger or banking Trojan. "I think that what we see here is the productization or even industrialization of malware techniques," says Tom Nipravsky, security researcher at Deep Instinct.

That industrialization aspect fits with what Solomon sees as the driving force behind this new malware. "It always comes down to money," he says. And that's especially true given one of Mylobot's behaviors: It seeks out and shuts down competing botnet software.

"We see the capability to make sure you have no competition," Solomon says, noting that in the highly unregulated world of malware, having more infected systems at your disposal than the competition can offer might be a matter of millions of dollars.

Mylobot leverages several techniques to make sure no other botnet is active on a machine it infects. "Usually we see this behavior when malware tries to shut down defensive software," Solomon notes. "In this case, it's fighting against its competition."

Though the researchers have been looking at Mylobot for several weeks, they aren't yet ready to say who the author is. There are some clues, though, including the fact that Mylobot scans for keyboard layout of an infected machine and doesn't execute if it finds an Asian character set and layout in use. Nipravsky says this could have to do with encryption algorithms, but it might well speak to the geographical nexus of the malware.

The researchers say it's important to note that Mylobot was found in the wild, at a Tier 1 data communication and telecommunication equipment manufacturer, not in a proof-of-concept demonstration.

"It's a relatively good representative of what we see on the Dark Web where people are selling platforms for others to use," Solomon says. Customers of the botnet can rent time to download and run their own payloads, making this a very efficient use of malware technology.

Read the rest here:
The Defense Department will, as a general rule, have to comply with new Homeland Security Department rules aimed at improving civilian government cybersecurity under the Senate’s version of a must-pass defense policy bill.

Homeland Security has issued a slew of the rules, known as binding operational directives, since the Trump administration took office, including banning the Moscow-based Kaspersky anti-virus from government systems and mandating anti-spoofing email security tools.

Right now, though, the binding operational directives are only binding on civilian agencies.

The Senate’s version of the National Defense Authorization Act specifically directs the Defense Department to implement the anti-spoofing email security directive. If the provision makes it into law, the department will follow the same three-month schedule to implement the tool, known as DMARC, that civilian government did.

DMARC, which stands for Domain-based Message Authentication, Reporting and Conformance, essentially pings a sender’s email domain and asks if the sender is legitimate. If the domain says the sender is illegitimate, DMARC can send the email to the recipient’s spam folder or decline to deliver it entirely.

As of February, about 38 percent of federal email domains had not yet implemented the anti-spoofing tool, though most of the government’s largest email domains were compliant, officials said.

For future Homeland Security directives, the Defense Department chief information officer must “notify the congressional defense committees within 180 days...whether the Department of Defense will comply with the directive or how the Department of Defense plans to meet or exceed the security objectives of the directive,” according to the text of the bill.

Read the rest here:

The U.S. House of Representatives on Monday passed a bill aimed at protecting industrial control systems (ICS), particularly ones used in critical infrastructure, against cyberattacks.

The legislation, H.R. 5733, formally known as the “DHS Industrial Control Systems Capabilities Enhancement Act," was introduced on May 9 by Rep. Don Bacon (R-NE) and it was approved by the House Committee on Homeland Security on June 6. The bill was announced a few weeks after the United States officially accused Russia of attempting to take control of critical infrastructure systems.

The new bill amends the Homeland Security Act of 2002 and requires the DHS’s National Cybersecurity and Communications Integration Center (NCCIC) to identify and mitigate threats and risks to ICS technologies and products used in critical infrastructure organizations.

The bill also requires NCCIC to maintain cross-sector incident response capabilities for ICS-related events, and provide technical assistance to end-users, product manufacturers, and other stakeholders in identifying and mitigating vulnerabilities in industrial control systems.

The agency is also required to provide the ICS community information on vulnerabilities based on collaboration with security researchers, manufacturers and industry end-users. The DHS will have to brief Congress every six months over the next four years.

The Congressional Budget Office (CBO) estimates that enacting this piece of legislation would cost less than $500,000 over the 2019-2023 period due to the fact that NCCIC already provides assistance to critical infrastructure operators and control system vendors, and the bill would only codify the agency’s responsibilities without imposing any new operating requirements.

Read the rest here:
https://www.icscybersecurityconference.com/u-s-house-passes-bill-to-enhance-industrial-cybersecurity/
25% of employees use the same password for every account

By Alison DeNisco Rayome, Tech Republic, June 11, 2018

Employees may be a company’s greatest asset, but they also remain the greatest cybersecurity risk, according to a Monday report from OpenVPN.

Despite an increased focus on security training, 25% of the 500 US employees surveyed report that they use the same password for every account, the report found. Another 23% of employees said they frequently click on links before verifying that they lead to a legitimate, safe website.

Of the employees that use the same password for everything, a whopping 81% said they do not password protect their computer or phone at all, according to the report.

"Cybersecurity breaches are a matter of 'when' not 'if,' and organizations have to be ready to address hackers head on," according to a blog post detailing the survey findings. "But with businesses so focused on external threats, they often overlook the role their own employees play in exposing vulnerabilities from inside an organization.

It should go without saying that reusing passwords is a risky behavior that can put an entire company at risk, as weak passwords can be more easily bypassed with brute force attacks. It can also cause damage to the individual, as using the same password to protect bank accounts, email, and social media can risk compromising both personal and work information, the post noted.

Traditional password best practices have recently changed: For example, the requirement of using a letter, a number, an uppercase, and a special character isn’t useful, and neither is the recommendation of changing your password every 90 days, according to Bill Burr, who published past password standards.

Instead, long, easy-to-remember phrases make the best passwords, Burr said. It is also recommended that users only be required to change their password if a breach has been suspected or confirmed.

Some employers are turning to biometric passwords such as fingerprints to enhance cybersecurity, the report found. These have generally been welcomed by employees: 77% said they trust biometric passwords, and 62% said they believe they are stronger than traditional alphanumeric codes, according to the survey. However, at this point, only about half of employees (55%) use biometric passwords.

Companies can protect their employees by creating a cyber hygiene routine that encourages workers to proactively think about their choices online, the post noted. Continuous security education and clear communication policies should be implemented at all organizations. Along with that, employers can promote positive reinforcement when employees make smart decisions, so that there is less fear to report cyber attacks. Instead of using scare tactics to warn about phishing or weak passwords, employers can think about rewarding or acknowledging individuals who embrace strong cyber hygiene.

Read the rest here:
https://www.techrepublic.com/article/25-of-employees-use-the-same-password-for-every-account/
A new data breach may have exposed personal information of almost every American adult

By Mike Murphy, Market Watch, June 28, 2018

A little-known Florida company may have exposed the personal data of nearly every American adult, according to a new report.

Wired reported Wednesday that Exactis, a Palm Coast, Fla.-based marketing and data-aggregation company, had exposed a database containing almost 2 terabytes of data, containing nearly 340 million individual records, on a public server. That included records of 230 million consumers and 110 million businesses.

"It seems like this is a database with pretty much every U.S. citizen in it," security researcher Vinny Troia, who discovered the breach earlier this month, told Wired. "I don't know where the data is coming from, but it's one of the most comprehensive collections I've ever seen," he said.

While the database apparently does not include credit-card numbers or Social Security numbers, it does include phone numbers, email and postal addresses as well as more than 400 personal characteristics, such as whether a person is a smoker, if they own a dog or cat, their religion and a multitude of personal interests. Even though no financial information was included, the breadth of personal data could make it possible to profile individuals or help scammers steal identities.

Troia told Wired that he was easily able to access the database on the internet, and in theory, plenty of other people could have too. He said he warned Exactis and the FBI about the vulnerability, and the data is no longer publicly accessible.

On its website, Exactis said it maintained 3.5 billion consumer, business and digital records, including "demographic, geographic, firmographic, lifestyle, interests, CPG, automotive, and behavioral data." The company said it has data on 218 million individuals and 110 million U.S. households.

There are about 325 million residents in the U.S., with about 244 million adults and 126 million households, according to the U.S. Census Bureau.

Exactis did not immediately respond when asked to confirm the breach.

If confirmed, the data leak would be one of the largest in history, and far bigger than the Equifax data breach last year that exposed the personal information of about 148 million consumers.

A 2016 breach of AdultFriendFinder exposed the data of more than 412 million accounts, while Yahoo’s 2013 hack exposed the personal data of about 3 billion accounts.

Read the rest here:
A volt out of the blue: Phone batteries reveal what you typed and read

By Richard Chirgwin, The Register, June 25, 2018

A group of researchers has demonstrated that smartphone batteries can offer a side-channel attack vector by revealing what users do with their devices through analysis of power consumption.

Both snitching and exfiltration were described in this paper (PDF), accepted for July's Privacy Enhancing Technologies Symposium.

Nobody needs to panic yet, because the attack isn't yet more than a decently tested theory, and it would be rather hard to execute. But there's also a real-world implication because the paper shows how a too-free API can help attackers in ways its designers never imagined.

The paper, by researchers from University of Texas in Austin, the Hebrew University of Jerusalem, and the Israel Institute of Technology explained that a “poisoned” battery can gather enough information about power-hungry phone components to reveal user activity.

In their research, the boffins turned a battery into a snitch by implanting a microcontroller to sample power flowing in and out at a 1kHz sample rate.

The battery, they wrote, is a very attractive attack vector because “all the phone activity is exposed.” An attacker can correlate power flows with a keystroke, the context of the keystroke (is someone visiting a website at the time?) and “the events that preceded or followed it,” such as taking a photo or making a phone call.

“Together, these pieces of information reconstruct a coherent portrait of the user’s activity, dramatically amplifying the power of individual attacks,” the paper states.

The authors contend that reading the CPU and screens’ power traces (and even those from the GPU or the DRAM in some cases) would reveal information about websites a user visited, or even what they were typing on the screen:

As an attack, it’s relatively clumsy. A miscreant would have to insert their poisoned battery – which is, however, feasible if you’ve had to hand a phone over to someone with legal authority or for repair. The attack also needs an offline AI to learn how to classify the power traces.

However, what's not theoretical is the exfiltration path – the Web Battery API, criticised as offering snitching options, and abandoned by Mozilla and Webkit for that reason.

Read the rest here:
https://www.theregister.co.uk/2018/06/25/the_battery_is_the_smartphones_ibesti_snitch_boffins/
Privacy, identity 'impossible to protect' say 74% of security pros

By Conner Forrest, TechRepublic, June 25, 2018

As more of daily life moves online, protecting personal identity and privacy becomes paramount. Unfortunately, it also may be impossible, according to 74% of cybersecurity professionals polled in a recent Black Hat survey.

Black Hat's "Where Cybersecurity Stands" report, announced in a Tuesday press release, gathered data from 300 security professionals. Their responses suggest that, even with "precautionary measures and new regulations such as GDPR," online privacy may be a lost cause. Roughly 30% said they didn't know if their organization met GDPR compliance, and 26% didn't think they were subject to it, according to the report.

As part of the survey, the respondents also weighed in on Facebook use. Some 55% of security pros said they advised their internal users to reconsider how much data they shared on the social media platform. Additionally, 75% of security pros said they were limiting their own use of Facebook, or giving it up entirely, the release said.

The respondents also expressed little faith in the White House's grasp of security issues, with a mere 13% of respondents saying they believed Congress and the White House understood current threats and how to protect against them in the future, the release noted. Respondents were more divided on the results of the 2016 presidential election, with 50% saying they thought Russian cyberattacks played a role in the outcome.

The Black Hat respondents were in favor of the prevalence of ethical hacking, with 90% saying they believed in the importance of coordinated disclosure, "making it clear that hackers within the Black Hat community are still looking to help in the fight against cyber crime," the release noted.

As far as the most effective tools to improve security, security pros picked the following three from a list of 18:

1. Encryption
2. Multi-factor authentication
3. Firewalls

According to the release, though, "passwords, one of the most widely used technologies, were dubbed ineffective by nearly 40% of respondents."

Read the rest here:
Server Virtualization Security: NIST Publishes SP 800-125A Revision 1

By Staff, NIST, June 7, 2018

Server Virtualization is now a key component for enterprise IT infrastructure in data centers and cloud services. Virtual servers provide better utilization of hardware resources, reduces physical space required for physical servers, and reduced power consumption as well. The core software used for server virtualization, the Hypervisor, directly provides CPU and memory virtualization.

The Hypervisor platform is a collection of software modules that provide virtualization of hardware resources, such as CPU, Memory, Network, and Storage, and enables computing stacks (operating systems and application programs) called Virtual Machines (VMs) to run on a single physical host. Additionally, the Hypervisor platform may have the functionality to define a network within a single physical host to enable communication among the VMs resident on that host, as well as with physical and virtual machines outside the host. The hypervisor has the responsibility to mediate access to physical resources, provide run time isolation among resident VMs, and enable a virtual network that provides a communication flow among the VMs and between the VMs and the external network.

To address additional technologies, NIST has published a revision of Special Publication (SP) 800-125A, now titled Security Recommendations for Server-based Hypervisor Platforms, which was originally published earlier this year. SP 800-125A Revision 1 adds security recommendations for technologies such as device passthrough and self-virtualizing devices that are used for deploying virtualized servers for high performance applications. The recommendations in this document relate to ensuring the secure execution of baseline functions of the hypervisor, ensuring they are agnostic to the hypervisor architecture. These recommendations are in context of a hypervisor deployed for server virtualization and not for other use cases such as embedded systems and desktops.

White House Reorganization Addresses Cyber Workforce Gap

By Jack Corregan, NextGox, June 21, 2018

The White House reorganization plan would force agencies to assess the strength of their cyber workforce and quickly fill the gaps they find.

The Trump administration on Thursday tasked the Homeland Security Department and Office of Management and Budget with creating a governmentwide approach for recruiting and retaining skilled cybersecurity personnel. The order, which came as part of the White House reorganization plan, aims to address the growing shortage of top cyber talent at federal agencies.

"The workforce shortage compounds the government’s challenges in responding to a constantly evolving threat environment and achieving its many IT-dependent missions," the report said. "The government lacks a comprehensive, risk-derived understanding of which cybersecurity skillsets the federal enterprise needs to develop and which positions are most critical to fill."

As it stands, each agency is responsible for addressing its own cybersecurity challenges, which the administration said creates “internal competition for talent... that degrade[s] agencies’ ability to defend networks from malicious actors and respond to cyber incidents.” The plan would standardize how agencies assess and meet their cyber needs.

Under the plan, the government would take stock of its entire cyber workforce by this fall using the framework created by the National Initiative for Cybersecurity Education. DHS would then work with agencies to assess their individual skill gaps and prioritize various hiring initiatives by the end of fiscal 2019.

Government has historically struggled to hire top tech professionals, but private sector’s growing demand for cyber talent compounded this problem. Today, the government employs almost five IT specialists over age 60 for each person under 30. A decade ago, the ratio stood slightly below two-to-one.

The private sector usually offers cyber specialists higher salaries and more career mobility than government, but the new approach looks to remove many of the obstacles that keep the best and brightest out of Washington.

Additional photographs are available on the ISSA-COS.ORG website
ISSA Photos are courtesy of our Chapter Photographer Warren Pearce.
The Information Systems Security Association (ISSA)® is a not-for-profit, international organization of information security professionals and practitioners. It provides educational forums, publications, and peer interaction opportunities that enhance the knowledge, skill, and professional growth of its members.

The primary goal of the ISSA is to promote management practices that will ensure the confidentiality, integrity, and availability of information resources. The ISSA facilitates interaction and education to create a more successful environment for global information systems security and for the professionals involved. Members include practitioners at all levels of the security field in a broad range of industries such as communications, education, healthcare, manufacturing, financial, and government.

Is Microsoft Doing the Right Thing by Killing the Windows Control Panel?

By Bogdan Popa, Softpedia, June 26, 2018

Microsoft declared war to the classic Control Panel back in July 2015 when it rolled out the first Windows 10 version, promising to move all options to Settings and eventually kill it off.

Three years later, the Windows Control Panel is still there, despite Microsoft moving more of its sections to the Settings app. Every new Windows 10 update represented a step forward in the migration from Control Panel to Settings, but in the April 2018 Update, both continue to be available.